Networked control of nonlinear systems under Denial-of-Service

De Persis, C.; Tesi, P.

Published in:
Systems & Control Letters

DOI:
10.1016/j.sysconle.2016.07.007

Publication date:
2016

Available online at www.sciencedirect.com

ScienceDirect

Systems & Control Letters 00 (2016) 1–13

Journal Logo

Networked Control of Nonlinear Systems under Denial-of-Service☆

C. De Persis*, P. Tesi

Engineering and Technology Institute Groningen (ENTEG) and the Jan Willems Center for Systems and Control, Faculty of Mathematics and Natural Sciences, University of Groningen, the Netherlands

Abstract

We investigate the analysis and design of a control strategy for nonlinear systems under Denial-of-Service attacks. Based on an ISS-Lyapunov function analysis, we provide a characterization of the maximal percentage of time that feedback information can be lost without resulting in instability of the system. Motivated by the presence of a digital channel we consider event-based controllers for which a minimal inter-sampling time is explicitly characterized.

1. Introduction

Motivated by interest in the analysis and control of critical infrastructures such as power networks, supply chains and transportation systems, recent years have witnessed increasing research interests in large-scale engineered systems. To achieve the prescribed control goal, these systems require exchange of information that often occurs in digital form. In turn this has triggered interest in control over communication channels. One of the topics that has stimulated broad interest is the so-called event-based control ([1]) in which sampling times are designed in real-time with the ultimate goal of saving communication resources while still guaranteeing the control goal. Event-based control has found fertile ground also in the area of cooperative control; *e.g.*, see [2, 3].

A natural research question raises when dealing with control over a communication channel: whether or not stability properties and performance are preserved in the presence of loss of feedback information. This loss of information could be due not only to malfunctioning but also to malicious actions by an adversarial entity [4, 5]. In the latter case, the assumption on the kind of information loss should be kept to a minimum since intelligent adversaries might not follow e.g. any statistical pattern. This aspect is in contrast with other work where the loss of information is mainly due to the unreliability of the communication channel [6].

Several contributions to the topic of stability/stabilization in the presence of adversarial entities have been reported in the last few years, with main emphasis on the so-called *Denial-of-Service* (DoS), a class of attack strategies primarily intended to affect the timeliness of information exchange [7]. In [4, 8], the authors address the problem of security constrained optimal control for discrete-time linear systems in which packets may be jammed by a malicious adversary, and the goal is to find optimal control and attack strategies assuming a maximum number of jamming

☆This work is partially supported by the Dutch Organization for Scientific Research (NWO) under the auspices of the project QUICK (QUantized Information Control for formation Keeping) and by the Research programme Robust Design of Cyber-physical Systems, financed by the Dutch Technology Foundation STW.

*Corresponding author

Email addresses: c.de.persis@rug.nl (C. De Persis), p.tesi@rug.nl (P. Tesi)

actions over a prescribed (finite) control horizon. Similar scenarios are considered in [9], where the problem of stabilizing a discrete-time linear system under DoS is casted as a dynamic zero-sum game, and in [10] where the authors investigate the problem of designing optimal attack schedules to maximize the expected average estimation error at the remote estimator.

An alternative scenario is addressed in [11], where the authors consider the problem of stability under *periodic* DoS for linear sampled-data systems under state-feedback. The idea there is to identify the jamming signal so as to restrict the information exchange to the time intervals where no DoS occurs. This approach has been then extended in [12] by considering energy-constrained, but otherwise *unknown* DoS attacks.

In [13], we addressed afresh the problem of stability under energy-constrained, but unknown, DoS attacks within the framework of linear sampled-data systems under state-feedback. Our work differs in many aspects from the aforementioned papers: in [4, 8, 9, 10], the authors consider a pure discrete-time setting, while here we deal with sampled-data networked systems and the performance analysis is concerned with the continuous-time process state. Second, we do not formulate the problem as an optimal control design problem. The controller can be designed according to any suitable design method, robustness against DoS attacks being achieved thanks to the design of the network transmission times. Finally, we focus on nonlinear systems. Our work also differs from the one in [11, 12] since the goal is not to identify the jamming signal; rather, the goal is to determine if stabilization is possible assuming only a bound on the fraction of the time the jammer is active. The considered approach, inspired by [1], consists in a suitable logic that determines in real-time the frequency of controller updates (the sampling times) depending on the DoS occurrence. In particular, the controller in [13] enjoys the following features:

i) It ensures *global* exponential stability of the closed-loop system whenever the intervals over which communication is possible are predominant with respect to the intervals over which communication is denied;

ii) It allows for the state-feedback control to be designed in accordance with any control design method, robustness against DoS being achieved thanks to the sampling logic;

iii) It is *resilient* since the sampling rate varies depending on the DoS occurrence;

iv) It allows for an explicit characterization of convergence rate, minimal inter-sampling time, and ratios between the "active" and "sleeping" periods of DoS which do not destroy closed-loop stability;

v) It is flexible enough so as to allow the designer to choose from several implementation options that can be used to trade-off performance vs. communication resources.

The objective of this paper is to put forward the investigation of similar ideas for nonlinear systems. Although we follow the line of arguments of [13], a few of the steps we take are very peculiar to nonlinear systems, making the extension far from straightforward and deserving attention on its own right. It is shown that under certain additional conditions, which are needed to avoid finite-escape times phenomena during DoS, *asymptotic stability* can be still ensured. The analysis combines elements from event-based control and ISS control Lyapunov functions.

A preliminary version of the paper was presented in [14]. Compared with the latter, this paper has undergone a major reorganization of the arguments and provides a complete version of all the proofs. One of the ideas on which the results are derived, namely taking into account in the analysis the switching between stable and unstable modes is not new and has been studied for both linear [15] and nonlinear systems [16]. We stress that the main novelty of our results, which makes our contribution profoundly different from previous work, lies in the design of an event-based resilient control strategy and in the explicit characterization of the intervals during which stable and unstable modes are active as a consequence of the DoS status.

The remainder of this paper is organized as follows. In Section 2 we introduce the framework of interest and provide an overview of the problem. In Section 3, we describe the considered class of DoS attacks and provide some preliminary stability results. The main result with a characterization of the class of DoS signals under which stability is preserved is given in Section 4. In Section 5, we discuss the theoretical results as well as their practical implementation. An example is given in Section 6. Section 7 provides concluding remarks and outlines future research directions.

Notation: The notation for this paper is in the main standard. For a vector $x \in \mathbb{R}^n$, $\|x\|$ denotes Euclidean norm. Given a continuously differentiable function f, we denote by ∇f its gradient. A function $\alpha : [0, \infty) \to [0, \infty)$ is said to be of class $\mathcal{K}$ if it is continuous, strictly increasing, and $\alpha(0) = 0$. In addition, it is said to be of class $\mathcal{K}_\infty$ if $\alpha(s) \to \infty$ as $s \to \infty$. A function $\beta : [0, \infty) \times [0, \infty) \to [0, \infty)$ is said to be of class $\mathcal{KL}$ if $\beta(\cdot, t)$ is of class $\mathcal{K}$ for each fixed $t \geq 0$ and and $\beta(r, t)$ decreases to 0 as $t \to \infty$ for each fixed $r \geq 0$. Given two functions f and g, we denote by $f \circ g$ the composite function $f(g)$.

2. Framework

We consider nonlinear systems of the form

$$\dot{x} = f(x, u), \tag{1}$$

where $x \in \mathbb{R}^n$ is the state and $u \in \mathbb{R}^m$ is the control input. We assume that $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ is Lipschitz continuous on compacts and satisfies $f(0, 0) = 0$. We also assume that there exists a function $\psi : \mathbb{R}^n \to \mathbb{R}^m$, which is Lipschitz continuous on compacts and satisfies $\psi(0) = 0$, such that $u = \psi(x)$ renders the closed-loop system input-to-state stable (ISS) with respect to measurement errors e in the sense that there exist a C^1 function $V : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ and class $\mathcal{K}_\infty$ functions $\alpha_1, \alpha_2, \gamma$ such that

$$\begin{aligned} &\alpha_1(\|x\|) \leq V(x) \leq \alpha_2(\|x\|) \\ &\nabla V(x) f(x, \psi(x + e)) \leq -\lambda V(x) + \gamma(\|e\|), \end{aligned} \tag{2}$$

with $\lambda > 0$.

As shown in [17], the ISS property (2) does always hold whenever the closed-loop system is ISS in the classical sense [18].

The control action is implemented via a *sample-and-hold* device. In a *nominal* situation, given a sequence of times $\{t_k\}_{k\in\mathbb{N}_0}$, $t_0 := 0$, the control signal u is given by $\psi(x(t_k))$ for all $t \in [t_k, t_{k+1})$, where $k \in \mathbb{N}_0$. The mechanism that generates this sequence of times will be specified in the sequel. By nominal situation is meant that at each time t_k at which the actuator needs to update the control value, it correctly receives the sampled value $\psi(x(t_k))$. The focus of this paper is on a scenario that is different from the nominal one, namely one in which there might be times in the sequence $\{t_k\}_{k\in\mathbb{N}_0}$ at which the control signal cannot be updated since no information regarding $\psi(x(t_k))$ is received by the actuator. This loss of information can be caused by several factors, such as a defective communication channel or as a consequence of the action of an adversarial entity. Throughout the remainder of this note, we will refer to such a phenomenon as *Denial-of-Service* (DoS). Practical considerations will be discussed in some detail in Section 5.

Let $\{h_n\}_{n\in\mathbb{N}_0}$, $h_0 \geq 0$, represent the sequence of DoS *off/on* transitions, *i.e.*, the sequence of time instants where the network changes from nominal to DoS status. Along with $\{h_n\}_{n\in\mathbb{N}_0}$, we consider a sequence $\{\tau_n\}_{n\in\mathbb{N}_0}$, $\tau_n \geq 0$, which specifies the duration of the n-th DoS status. Accordingly, we let

$$H_n = \{h_n\} \cup [h_n, h_n + \tau_n[\tag{3}$$

represent the n-th DoS time-interval. We assume that, during DoS, the actuator generates an input that is based on the *most recently received* control signal. A very similar analysis can be carried out in case the zero-input strategy is considered [6]. Given $t \in \mathbb{R}_{\geq 0}$, we denote by $\Theta(t)$ the set of all successful transmissions over the interval $[0, t]$. The control signal applied to the process at each time can be therefore expressed in compact form as

$$u(t) = \psi(x(t_{k(t)})) \tag{4}$$

where

$$k(t) := \begin{cases} -1, & \text{if } \Theta(t) = \emptyset \\ \sup\{\, k \in \mathbb{N} \mid t_k \in \Theta(t) \,\}, & \text{otherwise} \end{cases}. \tag{5}$$

Notice that $h_0 = 0$ implies $k(0) = -1$, which raises the question of assigning a value to the control input when communication is not possible at the process start-up. In this respect, we assume that when $h_0 = 0$ then $u(0) = 0$, and we let $x(t_{-1}) := 0$ for notational consistency.

2.1. Problem overview

The problem of interest is that of finding sampling logics that preserve stability despite the occurrence of DoS periods, while ensuring inter-sampling times bounded away from zero. In this respect, the result to follow will be centered around the following definitions.

Definition 1. *System Σ composed of (1) in closed-loop with (4) is said to have a* globally asymptotically stable *(GAS) origin if there exists a function β of class $\mathcal{KL}$ such that $\|x(t)\| \leq \beta(\|x(0)\|, t)$ for all $t \in \mathbb{R}_{\geq 0}$ and all $x(0) \in \mathbb{R}^n$.* ■

Definition 2. *Consider system Σ composed of (1) in closed-loop with (4). Σ is said to have a* finite δ-rate *if for any δ there exists a positive number $\varepsilon_\delta = \underline{\varepsilon}(\mathcal{B}_\delta) \in \mathbb{R}_{>0}$, with $\mathcal{B}_\delta$ the open ball of radius δ centered around the origin, such that, for any solution to Σ that belongs to $\mathcal{B}_\delta$, it holds that $\Delta_k := t_{k+1} - t_k \geq \varepsilon_\delta$ for all $k \in \mathbb{N}_0$.* ■

By "solution to Σ" we mean any absolutely continuous function x satisfying $\dot{x}(t) = f(x(t), \psi(x(t_{k(t)})))$ for almost all $t \in \mathbb{R}_{\geq 0}$ in some maximal interval of definition. Later, we will impose conditions on f, ψ, α_1 and γ so that the solutions exist globally for positive time [19].

3. Preliminary analysis

In this section, we provide a preliminary analysis of the problem under consideration along with some intermediate results.

3.1. Standing assumptions

In general, the uncontrolled system (1) (*i.e.*, with $u = 0$) might have unstable dynamics and also exhibit finite-escape times. This indicates two facts: (i) the duration of a DoS cannot be arbitrarily large; and (ii) conditions on the process dynamics must make sure that no finite-escape time occurs whenever the system evolves under out-of-date control samples.

As for (i), the main question to be addressed is that of determining the amount of DoS that a system can tolerate before undergoing instability. In this respect, it is simple to see that such an amount is not arbitrary, and that suitable conditions must be imposed on both DoS frequency and duration. As for the former, it is straightforward to verify that if the rate of DoS *off/on* transitions is allowed to be arbitrary, then stability can be lost irrespective of the sampling logic adopted because all communication attempts can be denied, no matter how fast is the sampling rate. Likewise, in order to get stability, the duration of the DoS status must be a suitable fraction of time. The following assumptions formalize the foregoing considerations. It is worth noting that such conditions do only constraint DoS frequency and duration in an average sense. No conditions are instead imposed on the DoS "structure": DoS is allowed to occur aperiodically, and the duration of any two different DoS intervals need not be equal to one another.

Assumption 1. *(*DoS frequency*). Let $n(t)$ denote the number of DoS* off/on *transitions on the semi-open interval $[0, t[$. There exist $\eta \in \mathbb{R}_{\geq 0}$ and $\tau_D \in \mathbb{R}_{>0}$ such that*

$$n(t) \leq \eta + t/\tau_D \tag{6}$$

for all $t \in \mathbb{R}_{\geq 0}$. ■

Assumption 2. *(*DoS duration*). Let $\Xi(t) := \bigcup_{n \in \mathbb{N}_0} H_n \bigcap [0, t]$ denote the total interval of DoS over $[0, t]$. There exist $\kappa \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{>1}$ such that*

$$|\Xi(t)| \leq \kappa + t/T \tag{7}$$

for all $t \in \mathbb{R}_{\geq 0}$. ■

Remark 1. *In Assumption 1, the term "frequency" stems from the fact that τ_D provides a measure of the dwell-time between any two consecutive DoS intervals. In particular, (6) yields a bound on the "average" dwell-time between consecutive DoS intervals, in agreement with the notion introduced in [20]. This property is ensured by the term η. In fact, this term allows for DoS to occasionally occur at a rate faster than $1/\tau_D$; however, when t is sufficiently large (hence t/τ_D is predominant compared with η) then the frequency of DoS is upper bounded by $1/\tau_D$. Assumption 2 provides a natural counterpart of Assumption 1 with respect to the DoS duration. In particular, in Assumption 2, the term "duration" refers to the fact that $1/T$ provides a measure of the fraction of time over which communication is denied (fraction since $T > 1$). Like η, the constant κ plays the role of a regularization term so that t/T should be interpreted as "average" DoS duration. The considered assumptions make it possible to capture many different types of DoS attacks. A discussion on this point is given in Section 5.2.* ■

As for (ii), the assumptions that follow guarantees that, whenever the process evolves under out-of-date control due to DoS, the trajectories cannot blow up in a finite time. A formal proof of this implication is given in Section 3.3 (Lemma 2), where it shown that under Assumption 3 and 4 the growth of V is always at most exponential. It is worth noting that such assumptions are always satisfied when the process dynamics are linear.

Assumption 3. *The functions f, ψ, and $\alpha_1^{-1} \circ \gamma$ are Lipschitz continuous on compacts.* ∎

Assumption 4. *There exists $\mu \in \mathbb{R}_{>0}$ such that*

$$\gamma(4r) \leq \mu\alpha_1(r) \tag{8}$$

for all $r \in \mathbb{R}_{\geq 0}$. ∎

3.2. Sampling logic

Given the stated assumptions, one expects that stability is not destroyed if the intervals over which communication is possible are predominant with respect to the intervals over which communication is denied. However, proving this fact is far from straightforward within the classical framework of nonlinear sampled-data systems [21, 22, 23, 24]. As shown next, the use of *aperiodic* sampling strategies as introduced in [1] provides a convenient framework to work with, in terms of both ease of analysis and effectiveness. As will become clear in the sequel, modifications to the strategy considered in [1] turn out to be necessary in order to account for the presence of DoS.

Consider system (1) in closed-loop with (4). Let

$$e(t) := x(t_{k(t)}) - x(t), \quad t \in \mathbb{R}_{\geq 0} \tag{9}$$

be the measurement error induced by the sampling. By hypothesis u renders the closed-loop ISS and, hence, satisfies the second of (2) with respect to e in (9). Consider next the following (prototypical) sampling logic:

1) *Sampling mode under nominal status.* If t_k does not belong to a DoS interval, then the next sampling instant t_{k+1} is defined as
$$\inf\{t > t_k : \gamma(4\|e(t)\|) > \lambda(1-c)V(x(t))\}, \tag{10}$$
where $c \in]0, 1[$;

2) *Sampling mode under DoS status.* If t_k belongs to some DoS interval, then the next sampling instant is defined as any t_{k+1} satisfying
$$\Delta_k \in [\underline{\Delta}, \bar{\Delta}], \tag{11}$$
where $\underline{\Delta} \in \mathbb{R}_{>0}$ and $\bar{\Delta} \in \mathbb{R}_{\geq \underline{\Delta}}$.

Following [1], it is straightforward to verify that, in the absence of DoS, sampling mode 1) guarantees that Σ has a GAS origin (*cf.* next Lemma 2). This can be indeed seen from the fact that (10) induces a dissipation inequality in the second of (2). However, in the presence of DoS, inequality $\gamma(4\|e\|) \leq \lambda(1-c)V(x)$ can be violated, and $\{t_k\}_{k\in\mathbb{N}_0}$ can result in an accumulation point. Sampling mode 2) is precisely introduced so as to avoid this situation, where $\underline{\Delta}$ is strictly positive in order to ensure that the inter-sampling times are bounded away from zero.

3.3. Key lemmas

Implementation details and variants of this sampling logic will be discussed in Section V. At this stage, it is convenient to focus the attention on the properties of the sampling logic that are central to the stability analysis. To begin with, we consider the δ-rate property of the closed-loop system. We then provide a characterization of the behavior of the Lyapunov function under nominal and DoS status, respectively. These two properties will be exploited in Section IV to analyze the overall closed-loop behavior.

Lemma 1. *Let Σ be the control system composed of (1) and (4), where the sampling instants are generated by (10)-(11). Suppose that Assumption 3 holds true. For any given $\delta \in \mathbb{R}_{>0}$, let L_δ be the Lipschitz constant of $f_\psi : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$ on $\mathcal{B}_\delta \times \mathcal{B}_{2\delta}$, where $f_\psi(x, e) = f(x, \psi(x + e))$, and let M_δ be the Lipschitz constant of $g : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ on $\mathcal{B}_{2\delta}$, where*

$$g(v) := \alpha_1^{-1}\left(\frac{1}{\lambda(1-c)}\gamma(4\|v\|)\right). \tag{12}$$

Then, Σ has a finite δ-rate given by

$$\varepsilon_\delta = \min\{\underline{\Delta}, 1/(L_\delta(1 + M_\delta))\}.$$

Proof. Consider any interval $[0, \tau]$, $\tau \in \mathbb{R}_{\geq 0}$, for which the solution to Σ belongs to $\mathcal{B}_\delta$. Pick any $t_k \in [0, \tau]$. Suppose first that t_k belongs to a DoS interval. It follows from (11) that $\Delta_k \geq \underline{\Delta}$. Suppose next that t_k does not belong to a DoS interval. Since by hypothesis $x \in \mathcal{B}_\delta$, then $e \in \mathcal{B}_{2\delta}$. In addition, $\|g(e)\| \leq M_\delta\|e\|$ for all $e \in \mathcal{B}_{2\delta}$. Hence, the next sampling time t_{k+1} generated by (10) is not smaller than the sampling time that would be generated by the triggering rule $\inf\{t > t_k : M_\delta\|e(t)\| > \|x(t)\|\}$. Along the same lines as in [1, Theorem III.1], Assumption 3 guarantees that $\Delta_k \geq 1/(L_\delta(1 + M_\delta))$. This concludes the proof. ∎

As for the characterization of the Lyapunov function under nominal and DoS status, we have the following result.

Lemma 2. *Let Σ be the control system composed of (1) and (4), where the sampling instants are generated by (10)-(11). Suppose that Assumptions 3 and 4 hold true. Also suppose that the solution to Σ exists up to a certain sampling time t_k, where $k \in \mathbb{N}_0$. Then, the solution to Σ exists up to t_{k+1}. Moreover, the Lyapunov function is such that:*

i) If t_k does not belong to a DoS interval,

$$V(x(t)) \leq e^{-\omega_1(t-t_k)}V(x(t_k)) \tag{13}$$

for all $t \in [t_k, t_{k+1})$, where $\omega_1 := c\lambda$;

ii) If t_k belongs to a DoS interval,

$$V(x(t)) \leq e^{\omega_2(t-t_{k(t_k)+1})}V(x(t_{k(t_k)+1})) \tag{14}$$

for all $t \in [t_{k(t_k)+1}, t_{k+1})$, where $\omega_2 := \lambda(1 - c) + 2\mu$.

Proof. First notice that a sufficient condition for the existence of the solutions up to t_{k+1} is that: i) there exists a positive constant ϵ such that $\Delta_k \geq \epsilon$; and ii) the solutions have no finite-escape time over $[t_k, t_{k+1}[$. Assume first that t_k does not belong to a DoS interval. Hence, it follows from (10) that (13) holds true for all $[t_k, t_{k+1})$. Moreover, since the solution exists up to t_k, then $x(t_k)$ is finite, and $\|x(t)\| \leq \alpha_1^{-1}(V(x(t_k)))$ for all $[t_k, t_{k+1}[$. By Lemma 1, this implies that $\Delta_k \geq 1/(L_\delta(1 + M_\delta))$, where $\delta := \alpha_1^{-1}(V(x(t_k)))$.

Assume next that t_k belongs to a DoS interval. In this case we have $\Delta_k \geq \underline{\Delta}$ by construction. We now prove (14). First notice that the claim trivially holds if $k(t_k) = -1$, *i.e.*, if no successful sampling occurred up to time t_k. In fact, under such circumstances, the second of (2) yields

$$\dot{V}(x(t)) \leq -\lambda V(x(t)) + \gamma(\|x(t)\|)$$

for all $t \in [0, t_{k+1})$. By Assumption 4 and the first of (2) we then have $\gamma(\|x(t)\|) \leq \mu V(x(t))$. The claim follows simply by noting that $-\lambda + \mu < -\lambda c + \mu < \omega_2$. Suppose next that $k(t_k) \neq -1$, *i.e.*, a successful sampling occurred before t_k. By construction,

$$\|e(t)\| \leq \frac{1}{4}\gamma^{-1}(\lambda(1 - c)V(x(t))) \tag{15}$$

for all $t \in [t_{k(t_k)}, t_{k(t_k)+1}]$, where $t_{k(t_k)+1}$ is included by continuity of V and the fact that also e is continuous at $t_{k(t_k)+1}$ because x is continuous and e is not reset at $t_{k(t_k)+1}$. We then have

$$\begin{aligned}
\|x(t_{k(t_k)})\| &\leq \|x(t_{k(t_k)+1})\| + \|e(t_{k(t_k)+1})\| \\
&\leq \|x(t_{k(t_k)+1})\| + \frac{1}{4}\gamma^{-1}(\lambda(1 - c)V(x(t_{k(t_k)+1}))) \\
&\leq \frac{1}{4}\gamma^{-1}(\mu V(x(t_{k(t_k)+1}))) \\
&\quad + \frac{1}{4}\gamma^{-1}(\lambda(1 - c)V(x(t_{k(t_k)+1})))
\end{aligned} \tag{16}$$

where the first inequality follows from the triangular inequality, the second inequality follows from (15), and the third inequality follows from the first of (2) and Assumption 4.

We can finalize the proof. Recall that, given a class $\mathcal{K}_\infty$ function γ and two non-negative reals a and b, it holds that $\gamma(a+b) \leq \gamma(2a) + \gamma(2b)$. Hence, bearing in mind that by definition $e(t) = x(t_{k(t_k)}) - x(t)$ for all $t \in [t_{k(t_k)}, t_{k+1})$,

$$\begin{aligned}\gamma(\|e(t)\|) &\leq \gamma(2\|x(t_{k(t_k)})\|) + \gamma(2\|x(t)\|)\\ &\leq (\lambda(1-c)+\mu)V(x(t_{k(t_k)+1})) + \gamma(2\|x(t)\|)\\ &\leq (\lambda(1-c)+\mu)V(x(t_{k(t_k)+1})) + \mu V(x(t))\end{aligned} \tag{17}$$

for all $t \in [t_{k(t_k)}, t_{k+1})$, where the second inequality follows from (16) and the property $\gamma(a+b) \leq \gamma(2a) + \gamma(2b)$, while the third inequality follows from Assumption 4.

By the second of (2) we then have $\dot{V}(x(t)) \leq \omega_2 \max\{V(x(t_{k(t_k)+1})), V(x(t))\}$, for all $t \in [t_{k(t_k)+1}, t_{k+1})$, from which (14) is proven. In fact, consider the differential *equation* $\dot{v}(t) = \omega_2 \max\{v(t_{k(t_k)+1}), v(t)\}$ over the interval $[t_{k(t_k)+1}, t_{k+1})$, with $v(t_{k(t_k)+1}) = V(x(t_{k(t_k)+1}))$. Then $v(t) = \mathrm{e}^{\omega_2(t-t_{k(t_k)+1})} v(t_{k(t_k)+1})$ for all $t \in [t_{k(t_k)+1}, t_{k+1})$, from which $V(x(t)) \leq \mathrm{e}^{\omega_2(t-t_{k(t_k)+1})} V(x(t_{k(t_k)+1}))$ as claimed.

■

4. Main results

The results of the previous section can be explained in words as follows: if a transmission is successful, then the Lyapunov function decreases until the next sampling (part i) of Lemma 2); if instead a transmission is not successful, then the Lyapunov function may increase, and a characterization of the growth of the Lyapunov function can be given directly in terms of consecutive unsuccessful transmissions (part ii) of Lemma 2). By Lemma 2, a quantification of the convergence/divergence rate is available in both cases. Overall, the closed-loop dynamics can be therefore viewed as those of a hybrid system which switches between stable and unstable modes.

Let $\{t_{k_m}\}_{m\in\mathbb{N}_0}$ be the subsequence of unsuccessful sampling times, and define

$$\Lambda(t) := \left(\bigcup_{m\in\mathbb{N}_0} [t_{k_m}, t_{k_m} + \Delta_{k_m}[\right) \cap [0,t]\,. \tag{18}$$

In words, $\Lambda(t)$ coincides with the set of time instants where the Lyapunov function may increase. Let now $\Lambda^c(t) := [0,t] \setminus \Lambda(t)$. By Lemma 2, we have that, as long as the solutions to Σ exist, the Lyapunov function satisfies

$$\begin{aligned}V(x(t)) &\leq e^{-\omega_1|\Lambda^c(t)|} e^{\omega_2|\Lambda(t)|} V(x(0))\\ &= e^{-\omega_1(t-|\Lambda(t)|)} e^{\omega_2|\Lambda(t)|} V(x(0))\end{aligned} \tag{19}$$

The problem is then that of finding conditions on the DoS under which the stable behavior is predominant with respect to the unstable one in the sense that x remains bounded. Under such circumstances, by Lemma 1, one also guarantees that the inter-sampling times are bounded away from zero, and, hence, that the solutions are forward complete.

We have the following result.

Lemma 3. *Let Σ be the control system composed of (1) and (4), where the sampling instants are generated by (10)-(11). Suppose that Assumptions 1 and 2 hold true. Then,*

$$|\Lambda(t)| \leq \kappa + \eta\bar{\Delta} + \left(1/T + \bar{\Delta}/\tau_D\right) t \tag{20}$$

for all $t \in \mathbb{R}_{\geq 0}$ such that the solutions to Σ exist.

Proof. Consider first all the intervals $[t_{k_m}, t_{k_m} + \Delta_{k_m}[$ for which there is a DoS *off/on* transition over $]t_{k_{m-1}}, t_{k_m}]$ as well as a DoS *on/off* transition over $[t_{k_m}, t_{k_m} + \Delta_{k_m}[$. Let $\alpha(t)$ denote their numbers over $[0,t[$. By (11), the total measure of these interval is therefore upper bounded by $\alpha(t)\bar{\Delta}$. Consider next all the remaining intervals. These intervals can be

grouped into *macro* intervals of the type $[t_{k_m}, t_{k_q} + \Delta_{k_q}[$ for which there is a DoS *off/on* transition over $]t_{k_{m-1}}, t_{k_m}]$ as well as a DoS *on/off* transition over $[t_{k_q}, t_{k_q} + \Delta_{k_q}[$. The number of these macro intervals over $[0, t[$ is necessarily bounded by $n(t) - \alpha(t)$ because $n(t)$ is the total number of DoS *off/on* transitions over $[0, t[$. Hence, their total measure cannot exceed $(n(t) - \alpha(t))\bar{\Delta} + |\Xi(t)|$. This is because the length of each macro interval $[t_{k_m}, t_{k_q} + \Delta_{k_q}[$ is upper bounded by the length of the DoS interval covering $[t_{k_m}, t_{k_q}]$ plus the length of $[t_{k_q} + \Delta_{k_q}[$ which is upper bounded by $\bar{\Delta}$. Overall, we then have $|\Lambda(t)| \leq n(t)\bar{\Delta} + |\Xi(t)|$. Assumptions 1 and 2 yield the result. ∎

Combining Lemma 1-3, we obtain the following main result, which establishes existence and convergence of the solutions in the presence of DoS.

Theorem 1. *Let Σ be the control system composed of (1) and (4), where the sampling instants are generated by (10)-(11). Suppose that Assumptions 1-4 hold true. If the parameters τ_D in (6) and T in (7) satisfy*

$$\frac{1}{T} + \frac{\bar{\Delta}}{\tau_D} < \frac{c\lambda}{\lambda + 2\mu}, \tag{21}$$

then Σ has a GAS origin. In particular,

$$\|x(t)\| \leq \alpha_1^{-1}\left(\rho \mathrm{e}^{-\beta t}\alpha_2(\|x(0)\|)\right) \tag{22}$$

for all $t \in \mathbb{R}_{\geq 0}$, where

$$\rho := e^{(\kappa + \eta\bar{\Delta})(\lambda + 2\mu)}, \quad \beta := c\lambda - (\lambda + 2\mu)\left(\frac{1}{T} + \frac{\bar{\Delta}}{\tau_D}\right) \tag{23}$$

and the parameters λ, κ and μ are as in (2), (7) and (8), respectively. Furthermore, the sequence of sampling times is lower bounded by $\varepsilon_\delta = \min\{\underline{\Delta}, 1/(L_\delta(1 + M_\delta))\}$, where $\delta = \alpha_1^{-1}(\rho\alpha_2(\|x(0)\|))$.

Proof. Recalling that $\omega_1 = c\lambda$ and $\omega_2 = \lambda(1 - c) + 2\mu$, (19) and Lemma 3 yield $V(x(t)) \leq \rho e^{-\beta t} V(x(0))$. The lower bound on the sampling times (hence also the completeness of the solutions) follow directly from Lemma 1. ∎

We also consider a variant of Theorem 1, useful in the case in which, instead of information on the average duration τ_D of a DoS attack, information on its minimum duration is available.

Assumption 5. *There exists $\underline{\tau} \in \mathbb{R}_{\geq 0}$ such that $\tau_n \geq \underline{\tau}$ for all $n \in \mathbb{N}_0$.* ∎

Theorem 2. *Let Σ be the control system composed of (1) and (4), where the sampling instants are generated by (10)-(11). Suppose that Assumptions 2-4 and 5 hold true. If the parameters $\underline{\tau}$ and T in (7) satisfy*

$$\frac{1}{T}\left(1 + \frac{\bar{\Delta}}{\underline{\tau}}\right) < \frac{c\lambda}{\lambda + 2\mu}, \tag{24}$$

then the same conclusions as in Theorem 1 hold true with ρ and β replaced by $\tilde{\rho}$ and $\tilde{\beta}$, respectively, where

$$\tilde{\rho} := e^{(\bar{\Delta} + \kappa(1 + \bar{\Delta}/\underline{\tau}))(\lambda + 2\mu)}, \quad \tilde{\beta} := c\lambda - (\lambda + 2\mu)\frac{1}{T}\left(1 + \frac{\bar{\Delta}}{\underline{\tau}}\right) \tag{25}$$

Proof. Even by replacing Assumption 1 with Assumption 5, the bound $|\Lambda(t)| \leq n(t)\bar{\Delta} + |\Xi(t)|$ in Lemma 3 is still valid. Hence, the proof of Theorem 1 carries over directly to the present case by noting that, under Assumption 5, $n(t) \leq 1 + \lfloor |\Xi(t)|/\underline{\tau} \rfloor$. ∎

5. Discussion

In this section, we provide some comments on the main results, discuss implementation aspects and outline possible variants of the considered sampling logic.

5.1. Stability and sampling rate properties

In both Theorem 1 and 2, the condition under which stability is not destroyed has an intuitive explanation. Notice that since $c < 1$, then $c\lambda/(\lambda + 2\mu) < 1$. Hence, one must necessarily have $1/T < 1$. Such a constraint expresses the property that, on the average, the time instants over which communication is interrupted cannot exceed a certain *fraction* of time (the precise amount being dictated by the convergence and divergence rate during nominal and DoS status, respectively). The second constraint is that also the term $\bar{\Delta}/\tau_D$ in Theorem 1 or the term $\bar{\Delta}/(T\underline{\tau})$ in Theorem 2 must be strictly less than one. These constraints mean that DoS cannot occur as frequently as the sample rate adopted during the DoS status. Since $\bar{\Delta}$ is a design parameter, then robustness against DoS can be increased by decreasing $\bar{\Delta}$. Such a feature will be discussed in more detail in the next subsection.

DoS also affects the stability properties of the closed-loop system indirectly via the inter-sampling times. To see this, notice that in a nonlinear setting the minimum inter-sampling time typically depends on the Lipschitz constants of the system [21, 22, 23], in the sense that the inter-sampling time required to ensure stability decreases as the process state gets far from the origin. This practically results in a *feasibility* constraint on the process initial conditions, which must be compatible with the sample rate allowed by the communication medium. In the present context, this is evident from the fact that the minimum inter-sampling is given by $\varepsilon_\delta = \min\{\underline{\Delta}, 1/(L_\delta(1 + M_\delta))\}$, where

$$\delta = \alpha_1^{-1}(\rho\alpha_2(\|x(0)\|))$$

in case of Theorem 1 (as for Theorem 2, the formula is the same with ρ replaced by $\tilde{\rho}$). In practice, the set of feasible initial conditions is therefore the one for which ε_δ is not smaller than the minimum inter-sampling time allowed by the communication medium. Compared with the (classical) case where communication is always possible, one sees that DoS further restricts the set of feasible initial conditions via ρ. The latter, in fact, grows with the parameters η and κ that appear in Assumption 1 and 2. Hence, given a constraint on the sampling rate and a compact set $\mathcal{X}$ of initial conditions that are feasible in the nominal case, then $x(0)$ must lie in a suitable subset of $\mathcal{X}$ whenever η and/or κ are different from zero.

5.2. DoS modeling examples

The considered DoS model only constrains the attacker action in time by posing limitations on the frequency of DoS and its duration. Limiting the DoS frequency and duration, in addition to render the control problem meaningful, does also have a practical motivation. In fact, there are several provisions that can be taken in order to *mitigate* DoS attacks, including spreading techniques, high-pass filtering and encoding [25, 26, 27]. These provisions decrease the chance that a DoS attack will be successful, and, as such, limit in practice the frequency and duration of the time intervals over which communication is effectively denied. In this respect, the difference between Theorem 1 and 2 (or, equivalently between Assumption 1 and 5) is mainly dictated by the considered type of DoS. For the sake of simplicity, we restrict ourselves to the case of radio frequency (RF) jammers, although similar considerations can be made with respect to spoofing-like threats [28].

Constant jamming is one of the most common threats that may occur in a wireless network [29, 30]. By continuously emitting RF signals on the wireless medium, this type of jammer can lower the Packet Send Ratio (PSR) for transmitters employing carrier sensing as medium access policy as well as lower the Packet Delivery Ratio (PDR) by corrupting packets at the receiver. In general, the percentage of packet losses caused by this type of jammer depends on the Jamming-to-Signal Ratio and can be difficult to quantify as it depends, among many things, on the type of anti-jamming devices (if any), the possibility to adapt the signal strength threshold for carrier sensing, and the interference signal power, which may vary with time. In this respect, Theorem 1 provides a quite general level of abstraction since no constraint is posed on the DoS occurrence apart from the fact that it sufficiently slow in an average sense.

A different situation may arise with *reactive jamming* [29, 30]. By exploiting the knowledge of the 802.1i MAC layer protocols, a jammer may restrict the RF signal to the packet transmissions. The collision period need not be long since with many CRC error checks a single bit error can corrupt an entire frame. Accordingly, jamming takes the form of a (high-power) burst of noise, whose duration is determined by the length of the symbols to corrupt [26, 31]. In this situation, the DoS signal exhibits some structure and one can replace Assumption 1 and 5, where the parameter $\underline{\tau}$ is determined by the length of the symbols to corrupt.

5.3. Implementation: Event-based vs. time-triggered sampling logics over TCP/UDP-like channels

Event-based rules such as (10) require a continuous monitoring of the state of the process by the sensor. A possibility to avoid this is implementation is already suggested by Lemma 1 and 2. Specifically, let

$$\underline{k}(t) := \begin{cases} -1, & \text{if } \Theta(t) = \emptyset \\ \inf\{\, k \in \mathbb{N}_0 \mid t_m \in \Theta(t) \,, & \text{otherwise} \\ \qquad \text{for } m = k, k+1, \dots, k(t)\} & \end{cases} . \tag{26}$$

In words, $\underline{k}(t)$ denotes the smallest integer such that all the sampling instants within $[t_{\underline{k}(t)}, t_{k(t)}]$ are successful. A time-triggered logic can be therefore implementated as follows: at those sampling times t_k which do not belong to any DoS interval, the next sampling time is chosen as $t_{k+1} = t_k + \varepsilon_{\delta_k}$, where $\varepsilon_{\delta_k} = 1/(L_{\delta_k}(1 + M_{\delta_k}))$ and

$$\delta_k = \alpha_1^{-1}(\alpha_2(\|x(t_{\underline{k}(t_k)})\|))$$

On the other hand if a sampling occurs during a DoS interval, then $t_{k+1} = t_k + \Delta_k$, where $\Delta_k \in [\underline{\Delta}, \bar{\Delta}]$ and $\underline{\Delta}$ is any positive number larger than the minimal sampling period which the sampling device can provide. The rationale stems from the following facts: i) by Lemma 1, the inter-sampling $\varepsilon_\delta = 1/(L_\delta(1 + M_\delta))$ guarantees that the Lyapunov function is decreasing as long as the solutions remain within $\mathcal{B}_\delta$; and ii) by Lemma 2, in the absence of DoS, any solution starting within $\mathcal{B}_R$ remain within $\mathcal{B}_\delta$, where $\delta = \alpha_1^{-1}(\alpha_2(R))$. Overall, the sampling logic takes the form

$$t_0 = 0 \tag{27}$$

$$t_{k+1} = t_k + \begin{cases} \Delta_k, & \text{if } t_k \text{ belongs to a DoS interval} \\ \varepsilon_{\delta_k}, & \text{otherwise.} \end{cases} \tag{28}$$

The result above presents a precise characterization of time-triggered sampled-data stabilizing controllers for nonlinear systems under DoS, thus extending classical results on sampled-data stabilization under data loss. We note that, in contrast with the event-based implementation, the time-triggered implementation requires the computation of the Lipschitz constants L_{δ_k} and M_{δ_k} upon each sampling time. Nonetheless, this task can be easily accomplished since δ_k depends on $x(t_k)$ only via its magnitude. Hence, they can be precomputed off-line via a suitable state space gridding.

Both the event-based rule (10) and its time-triggered variant (28) rest on the hypothesis that it is possible to detect a DoS occurrence. If DoS consists in denying access to the communication medium (transmitters employing carrier sensing) this hypothesis can always be considered as true. If instead DoS consists in causing packet collisions at the receiver the validity of this hypothesis depends on the transport layer protocol. In acknowledgement-based protocols like the TCP, the DoS occurrence can be inferred from the lack of acknowledgement. In UDP-like protocols, however, the receiver does not generate an acknowledgement of packets received. Under such circumstances, neither (10) nor (28) can be implemented. A simple way to overcome this problem consists in letting $t_{k+1} = t_k + \varepsilon_{\delta_k}$, where ε_{δ_k} is always selected based on the value of the process state at the measurement instants. By the previous arguments, a possible choice for ε_{δ_k} is given by

$$\delta_k = \alpha_1^{-1}(\alpha_2(\|x(t_k)\|)) \tag{29}$$

Compared with (28), one sees that (29) potentially results in smaller inter-sampling periods. However, the latter has the advantage of not relying on the acknowledgement of packets received.

6. A numerical example

We consider the example in [32]. The nonlinear system of interest is given by

$$\dot{x} = x^2 - x^3 + u \tag{30}$$

The system is not GAS in open-loop. The stabilizing control law is $u = -2x$. We select $V(x) = \frac{1}{2}x^2$ as Lyapunov function, so that the first of (2) holds true with $\alpha_1(r) = \alpha_2(r) = \frac{1}{2}r^2$. As for the second of (2), notice that

$$\begin{aligned} \nabla V(x) f(x, \psi(x + e)) &= x(x^2 - x^3 - 2(x + e)) \\ &= x^3 - x^4 - 2x^2 - 2xe \\ &\le x^3 - x^4 - 2x^2 + cx^2 + \frac{1}{c}e^2 \end{aligned} \tag{31}$$

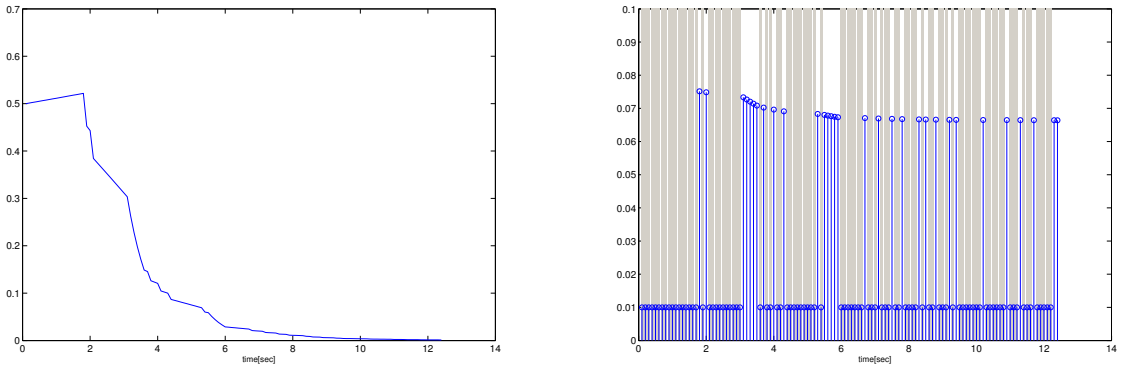

Figure 1. Simulation results for $x(0) = 0.5$ and a DoS signal generated randomly. Over a simulation horizon of 12s, the DoS signal yields $|\Xi(0, 12)| \approx 9$s and $n(0, 12) = 22$, and approximately 75% of transmission failures. In terms of Assumption 1 and 2, consistent DoS parameters are, for example, $(\eta, \kappa, \tau_D, T) = (1, 0.5, 0.54, 1.33)$. Left: State evolution; Right: Inter-sampling time (black). The vertical grey stripes represent the time-intervals over which DoS is active.

where the inequality follows from the Young's inequality, where c is any positive real. Letting $c = 3/4$ we obtain

$$\begin{aligned}\nabla V(x) f(x, \psi(x+e)) &\leq x^3 - x^4 - \frac{5}{4}x^2 + \frac{4}{3}e^2 \\ &\leq -x^2 + \frac{4}{3}e^2 \\ &= -2V(x) + \frac{4}{3}e^2 \end{aligned} \tag{32}$$

where the second inequality follows from the fact that $x^3 - x^4 - \frac{5}{4}x^2 + x^2 = -x^2(x^2 - x + \frac{1}{4}) = -x^2(x - \frac{1}{2})^2 \leq 0$. Hence, the second of (2) holds true with $\lambda = 2$ and $\gamma(r) = \frac{4}{3}r^2$. Moreover, Assumption 3 and 4 are trivially verified. In particular, Assumption 4 holds true with $\mu = 128/3$.

Using these parameters we can compute the DoS percentage under which GAS is preserved as well as lower bounds on the inter-sampling times. For instance, selecting $c = 0.5$ and $\underline{\Delta} = \bar{\Delta} = 0.01$ in the sampling logic (10)-(11) we obtain that stability is preserved as long as T and τ_D satisfy (*cf.* Theorem 1)

$$\frac{1}{T} + \frac{0.01}{\tau_D} < \frac{c\lambda}{\lambda + 2\mu} = \frac{3}{262} \approx 0.011 \tag{33}$$

We notice that this bound is conservative: as shown in Figure 1, the bound can in practice be much larger than the theoretical one. The conservativeness mainly comes from the bound on the growth of the Lyapunov function during the DoS, as this bound holds for *any* nonlinear system satisfying Assumption 3 and 4.

As for the lower bound on the inter-sampling times, we need to compute the constants M_δ and L_δ. As for M_δ, we immediately have

$$\begin{aligned} g(v) &= \alpha_1^{-1}\Big(\frac{1}{\lambda(1-c)}\gamma(4\|v\|)\Big) \\ &= \sqrt{2\gamma(4\|v\|)} = \sqrt{\frac{8}{3}16\|v\|^2} = \frac{8\sqrt{2}}{\sqrt{3}}\|v\| \end{aligned} \tag{34}$$

so that $M_\delta = \frac{8\sqrt{2}}{\sqrt{3}}$. As for L_δ, note that $f_\psi(x, e) = f(x, \psi(x + e)) = x^2 - x^3 - 2x - 2e$. Hence, for any $(x, e) \in \mathcal{B}_\delta \times \mathcal{B}_{2\delta}$ we obtain

$$\begin{aligned} |f_\psi(x, e)| &\leq \delta\|x\| + \delta^2\|x\| + 2\|x\| + 2\|e\| \\ &\leq 3\max\{\delta^2, 2\}\|x\| + 2\|e\| \end{aligned} \tag{35}$$

so that $L_\delta = 3\max\{\delta^2, 2\}$. Using these parameters we conclude that the lower bound on the inter-sampling times is given by

$$\varepsilon_\delta = \min\left\{0.01, \frac{1}{\max\{\delta^2, 2\}(3 + 8\sqrt{6})}\right\}$$

By Theorem 1, the trajectories always remain in the ball or radius $\delta = \alpha_1^{-1}(\rho\alpha_2(\|x(0)\|))$, where $\rho = e^{(\kappa+\eta\bar{\Delta})(\lambda+2\mu)} = e^{\frac{262}{3}(\kappa+0.01\eta)}$, so that $\delta = \sqrt{\rho\|x(0)\|^2} = e^{\frac{262}{6}(\kappa+0.01\eta)}\|x(0)\|$. Also in this case, the theoretical bounds are much more conservative than in practice.

7. Conclusions

The paper investigates the design of event-based control strategies for nonlinear systems in the presence of DoS attacks that interrupts the flow of information from the sensors to the actuators. The DoS signal attack is modeled at a fairly general level that we believe allows for the inclusion of several interesting scenarios. Relations between the sampling frequency, the data of the nonlinear systems under control and the features of the DoS attack signal have been revealed. The main working assumption is Assumption 4 whose role is to prevent the occurrence of finite escape times. It therefore restricts the class of nonlinear systems but allows for a less complicated analysis. Clearly, removing this assumption requires to restrict the class of DoS attacks the system can tolerate: if the systems undergoes prolonged attacks, it will evolve in open loop for long time intervals facing the possible occurrence of a finite escape time. This alternative formulation may be worth of investigation.

In future work, more attention will be given to the actual implementation of our resilient control and in particular to its connections with other event-based approaches such as self-triggered control. Relevant case studies to assess the effectiveness of our approach are also part of our future research plan. Whether our method can deal with attack scenarios different from DoS attacks is a topic worth of investigation as well. Robustness of the proposed resilient control (as well as of its linear counterpart studied in [13]) to external disturbances in an ISS sense is a very interesting and challenging research topic that can be tackled following e.g., the lines of arguments in [33]. Our initial interest for resilient control was motivated by distributed control strategies for dynamical networks in a cyberphysical environment (see e.g. [3]). We believe that our technique can be extended to distributed resilient control and can be a very fertile research ground.

References

[1] P. Tabuada, Event-triggered real-time scheduling of stabilizing control tasks, IEEE Transactions on Automatic Control 52 (2007) 1680–1685.
[2] G. Seyboth, D. Dimarogonas, K. Johansson, Event-based broadcasting for multi-agent average consensus, Automatica 49 (2013) 245–252.
[3] C. De Persis, P. Frasca, Robust self-triggered coordination with ternary controllers, IEEE Transactions on Automatic Control 58 (2013) 3024–3038.
[4] S. Amin, A. Càrdenas, S. Sastry, Safe and secure networked control systems under denial of-service attacks, In Hybrid systems: Computation and Control, (2009) 31–45.
[5] Y. Mo, T. Hyun-Jin Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber-physical security of a smart grid infrastructure, Proceedings of the IEEE 100 (2012) 195–209.
[6] L. Schenato, To hold or to zero control inputs with lossy links?, IEEE Trans. Autom. Control, 54 (2009) 1093–1099.
[7] E. Byres, J. Lowe, The myths and facts behind cyber security risks for industrial control systems, in: Proceedings of the VDE Congress, Berlin, 2004.
[8] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal dos attack scheduling in wireless networked control system, IEEE Transactions on Control Systems Technology (2015), In press DOI: 10.1109/TCST.2015.2462741.
[9] A. Gupta, C. Langbort, T. Başar, Optimal control in the presence of an intelligent jammer with limited actions, in: Proc. of the 49th IEEE Conference on Decision and Control, Atlanta, GA, USA, 2010.
[10] H. Zhang, P. Cheng, L. Shi, J. Chen, Optimal denial-of-service attack scheduling with energy constraint, IEEE Transactions on Automatic Control 60 (2015) 3023–3028.
[11] H. S. Foroush, S. Martínez, On event-triggered control of linear systems under periodic denial of service attacks, in: Proc. of the 51st IEEE Conference on Decision and Control, Maui, HI, USA, 2012.
[12] H. S. Foroush, S. Martínez, On triggering control of single-input linear systems under pulse-width modulated dos jamming attacks, SIAM Journal on Control and Optimization (2014), Submitted.
[13] C. De Persis, P. Tesi, Resilient control under denial-of-service, in: Proc. of the IFAC World Conference, Cape Town, South Africa, 2014.
[14] C. De Persis, P. Tesi, On resilient control of nonlinear systems under denial-of-service, in: Proc. of the 53rd IEEE Conference on Decision and Control, Los Angeles, CA, USA, 2014.

[15] G. Zhai, B. Hu, K. Yasuda, A. Michel, Stability analysis of switched systems with stable and unstable subsystems: An average dwell time approach, in: Proc. of the American Control Conference, Chicago, Illinois, 2000.
[16] M. Müller, D. Liberzon, Input/output-to-state stability and state-norm estimators for switched nonlinear systems, Automatica (2012) 2029–2039.
[17] L. Praly, Y. Wang, Stabilization in spite of matched unmodeled dynamics and an equivalent definition of input-to-state stability, Mathematics of Control, Signals and Systems 9 (1994) 1–33.
[18] E. D. Sontag, Input to State Stability: Basic Concepts and Results, Springer, Berlin, Heidelberg, 2008, pp. 163–220.
[19] A. Bacciotti, L. Rosier, Liapunov Functions and Stability in Control Theory (2nd edition), Communications and Control engineering, Springer Verlag, 2005.
[20] J. Hespanha, A. Morse, Stability of switched systems with average dwell-time, Proc. of the 38th IEEE Conference on Decision and Control, Phoenix, Arizona USA.
[21] D. Nešić, A. Teel, P. Kokotovic, Sufficient conditions for stabilization of sampled-data nonlinear systems via discrete-time approximations, Systems & Control Letters 38 (1999) 259–270.
[22] D. Nešić, D. Laila, A note on input-to-state stabilization for nonlinear sampled-data systems, IEEE Transactions on Automatic Control 47 (2002) 1153–1158.
[23] D. Nešić, A. Teel, A framework for stabilization of nonlinear sampled-data systems based on their approximate discrete-time models, IEEE Transactions on Automatic Control 49 (2004) 1103–1122.
[24] W. Bian, M. French, General fast sampling theorems for nonlinear systems, Systems & Control Letters 54 (2005) 1037–1050.
[25] W. Xu, K. Ma, W. Trappe, Y. Zhang, Jamming sensor networks: Attack and defense strategies, IEEE Network 20 (2006) 41–47.
[26] B. DeBruhl, P. Tague, Digital filter design for jamming mitigation in 802.15.4 communication, in: Int. Conference on Computer Communications and Networks, Maui, Hawaii, 2011.
[27] P. Tague, M. Li, R. Poovendran, Mitigation of control channel jamming under node capture attacks, IEEE Transactions on Mobile Computing 8 (2009) 1221–1234.
[28] J. Bellardo, S. Savage, 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions, in: Proceedings of USENIX Security Symposium, 2003.
[29] W. Xu, W. Trappe, Y. Zhang, T. Wood, The feasibility of launching and detecting jamming attacks in wireless networks, in: ACM International Symposium on Mobile Ad-Hoc Networking & Computing, 2005.
[30] K. Pelechrinis, M. Iliofotou, S. Krishnamurthy, Denial of service attacks in wireless networks: The case of jammers, IEEE Communications Surveys & Tutorials 13 (2010) 245–257.
[31] A. Wood, J. Stankovic, Denial of service in sensor networks, EEE Computer 10 (2002) 54–62.
[32] R. Postoyan, A. Anta, D. Nešić, P. Tabuada, A unifying Lyapunov-based framework for the event-triggered control of nonlinear systems, in: Proc. of the 50th IEEE Conference. on Decision and Control and European Control Conference., Orlando, USA, 2011.
[33] C. De Persis, P. Tesi, Input-to-state stabilizing control under denial-of-service, IEEE Transactions on Automatic Control 60 (11) (2015) 2930–2944.